An All-Hazard Approach for the Vulnerability Analysis of Critical Infrastructures

Enrico Zio, Roberta Piccinelli, Giovanni Sansavini

An All-Hazard Approach for the Vulnerability Analysis of Critical Infrastructures

E.Zio
Ecole Centrale Paris- Supélec, Paris, France, Politecnico di Milano
R.Piccinelli and G.Sansavini
Politecnico di Milano

ABSTRACT: In this paper, a framework is proposed for the *All-HAZard ANalysis* (A-HAZAN) of Critical Infrastructures (CIs). Starting from the identification of the task of each component in the infrastructure, we use tabular procedures to organize the information on the susceptibility to attacks, to single and cascading failures. All variables and states are identified that may impact on the component's role as a possible source of vulnerability within the CI and towards interdependent CIs. This is a starting point for a quantitative evaluation of the degree of exposure to intentional acts. A case study of literature is taken as an exemplary demonstration of the procedures of the analysis.

1 INTRODUCTION

Critical infrastructures (CIs) like the electricity, oil & gas supply, rail, road, air, sea transport, internet networks, are highly interconnected and mutually dependent in complex ways, both physically and through a multitude of information and communication technologies (so called cyber-based systems) used for data acquisition and control. The coupling of CIs leads to the concept of "systems-of-systems", which implies that single CIs cannot be studied in isolation from other CIs; rather, it is necessary to assess the limitations that interacting CIs pose on the operating conditions of the individual infrastructures so as to implement adequate protections for preventing failures in one CI from cascading to other dependent CIs.

The 2001 prolonged power crisis in California demonstrates the importance of coupling in interdependent CIs (Rinaldi et al., 2001). The crisis took place when electric power disruptions at various times curtailed natural gas production (first order effects); the latter generated a shutdown of steam injection in heavy oil production (second order effects).

A common denominator is needed to assess the vulnerability of a system that is exposed to natural and accidental hazards, and threats of malevolent acts. The need is to capture the CI vulnerability sources and issues, given its technical and physical features, and the dependencies and interdependencies on other systems. This requires an evaluation of the exposure to different hazards, including threats of malevolent acts.

An analysis aimed at identifying the causes of damage or disruption of services in CIs needs to embrace an *all-hazard approach* (Waugh, 2004), (Pollet and Cummins, 2009), encompassing a general view on the hazards targeting a given system.

We propose a framework for an *All-HAZard ANalysis* (A-HAZAN) which relies on tailored tabular procedures to organize the qualitative and quantitative features of the system relevant for revealing and highlighting its vulnerabilities. The A-HAZAN framework is intended as a tool for managers, analysts and stakeholders of CIs to carry out the identification of all the sources of vulnerability in an all-hazard perspective.

The paper is organized as follows. In Section 2, some methodologies to assess the vulnerabilities of CIs are reviewed. In Section 3, the concepts of vulnerability and susceptibility are outlined from the perspective of CIs. In Section 4, the A-HAZAN tabular procedure and a methodology are presented. In Section 5, the A-HAZAN methodology is applied to a literature case study. Conclusions are drawn in Section 6.

2. METHODOLOGIES OF VULNERABILITY ASSESSMENT

Screening methodologies for prioritizing scenarios of terrorist threats and identifying vulnerabilities in single and interdependent CIs have been proposed. Apostolakis and Lemon (Apostolakis and

Lemon, 2005) and Patterson and Apostolakis (Patterson and Apostolakis, 2007) focus on the identification of critical locations in infrastructures; these are seen as geographical points that are exposed to intentional attacks. Critical locations are not limited to individual infrastructures but may affect multiple infrastructures: for example, water and electrical distribution systems may occupy the same service tunnels. In the proposed scheme, the conditional probabilities that the terrorists will successfully exploit a vulnerability need to be evaluated. The procedure for this relies on extensive use of expert judgment and may be challenging in practice. The impacts of attacks are treated without including the probabilities of various levels of damage, and without consideration of any intervention by first responders: for this reason, it can be defined conservative. The vulnerabilities and their ranking according to potential impact are eventually obtained by Multi-Attribute Utility Theory (MAUT) (Morgan et al. 2000).

Konce et al. (Konce et al., 2008) have proposed a methodology for ranking components of a bulk power system with respect to its risk significance to the involved stakeholders; the likelihood and the extent of power outages when components fail to perform their designed functions are analyzed; the consequences associated with the failures are determined by considering the type and number of customers affected.

Johansson and Hassel (Johansson and H. Hassel, 2010) have proposed a framework for considering structural and functional properties of interdependent systems and developing a predictive model in a vulnerability analysis context. Piwowar et al. (Piwowar et al., 2009) have proposed a systemic analysis which accounts for malevolence, i.e., the willingness to cause damage.

The aim of the present work is to develop a systematic framework of system analysis for identifying the vulnerable elements of CIs, considering natural hazards, random failures and intentional attacks. While the first two types of vulnerability are characterized by stochastic uncertainties and can be analyzed by traditional safety analysis tools, intentional attacks require a new way of analysis.

3. HAZARDS, THREATS AND VULNERABILITY

In the United Nations' view, hazard is defined as "a potentially damaging physical event, phenomenon and/or human activity, which may cause loss of life or injury, property damage, social and economic disruption or environmental degradation. Hazards can be single, sequential or combined in their origin and effects" (Turner et al., 2003). The European Cooperation for Space Standardization (ECSS) defines hazard as "an existing or potential condition of an item that can result in an accident" (White, 1974); the condition is associated with the design, fabrication, operation or environment of the item, and has the potential for accidents. These two definitions encompass the idea of hazard described as a "condition prerequisite to a mishap" (UNISDR, 2004) and as "a source of potential harm" (ECSS, 2004). The concept of hazard is strictly tied to the presence of a potential source of difficulty both natural or manmade.

On the other hand, the concept of threat is defined as "a potential intent to cause harm or damage to the system by adversely changing its state" (ISO guide, 2009). This definition is strictly linked to intentional and malevolent acts (Apostolakis and Lemon, 2005), and it seems in contrast with the one by the US Homeland Security, which describes threat as a "natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property" (OHS, 2009). In the latter, little reference is made to the idea of intention embedded in the former definition of threat. From these definitions, the broader concept of hazard emerges as a general condition of potential source of harm. Therefore, it encompasses the intentionality of threats, e.g., terrorist acts that are distinguished by a malevolent intelligence directed toward maximum social disruption.

In the all-hazard approach, malevolent acts, accidental and natural occurrences are all considered. Yet, they require a different analytical treatment. Random accidents, natural failures and unintentional man-made hazards are typically known and categorized by emergency planners. Their occurrence can be typically addressed within a probabilistic framework (Figure 1). Conversely, terrorism is a hazard that eludes a quantification by probability theory due to the intentional and malevolent planning it implies (Figure 1).

Figure 1. All–Hazard Approach overview.

The concept of vulnerability follows the degree of impact that an hazard has on the CI. In (Konce et al., 2008), vulnerability is defined as "the degree to which a system, a subsystem or a system component is likely to experience harm due to exposure to a hazard, either a perturbation or stress" or, equivalently, in (Apostolakis and Lemon, 2005) as the "manifestation of inherent states of the system (e.g., physical, technical, organizational, cultural) that can be exploited by an adversary to harm or damage the system". Along the same line of thought, vulnerability is also defined as a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard (OHS, 2009). The United Nations define vulnerability as the conditions determined by physical, social, economic, and environmental factors or processes, which increase the susceptibility of a community to the impact of hazards (UNISDR, 2004).

Quantitatively, vulnerability focuses on three aspects (Konce et al., 2008):

- degree of losses and damages due to the impact of a hazard;
- degree of exposure to the hazards, i.e., likelihood of being exposed to hazards of a certain degree and susceptibility of an element at the risk of suffering losses and damages;
- degree of resilience, i.e., ability of a system to anticipate, cope with/absorb, resist and recover from the impact of a hazard or disaster.

Practically, vulnerability comes from flaws or weaknesses in the design, implementation, operation and management of an infrastructure that makes it susceptible to destruction or incapacitation when exposed to a hazard or threat, or reduces its capacity to resume stable conditions. For example, the vulnerability of the electric power system might be quantified in terms of changes in network characteristics following attacks on nodes, and the scale (e.g., number of nodes/lines lost) or duration of the associated losses. In a somewhat more intuitive interpretation, vulnerability characterizes a system component or an aspect of a system (Jönsson et al., 2008). A component is said to be a vulnerability of a system if its failure causes large negative consequences. In this sense, the component is said to be critical and the term vulnerability describes a property which can be employed for ranking the system's components with respect to their criticality.

Given the above, the goals of vulnerability analysis becomes then (Kroger and Zio, 2011):

1. identifying the set and sequences of events that cause damages and losses;
2. identifying the relevant set of "initiating events" and evaluate their cascading impact on a subset of elements, or the system as a whole;
3. determining and elaborating on (inter)-dependencies (within the system and among systems) and on coupling of different orders, given the set of initiating events and observed outcomes.

The ultimate goal is to identify obvious and, most important, hidden vulnerabilities in infrastructure systems to act for managing and reducing them. The achievement of these goals relies on the analysis of the system, of its parts and of their interactions. The analysis must account for the environment where the system operates, and for the objectives the system is designed to achieve. During the development of such basic system understanding, first vulnerabilities may already emerge.

In this paper, an *All-HAZard ANalysis* (A-HAZAN) framework is proposed to grasp the complementary aspects of random failures, or unintentional or natural occurrences, and malevolent attacks (Figure 2).

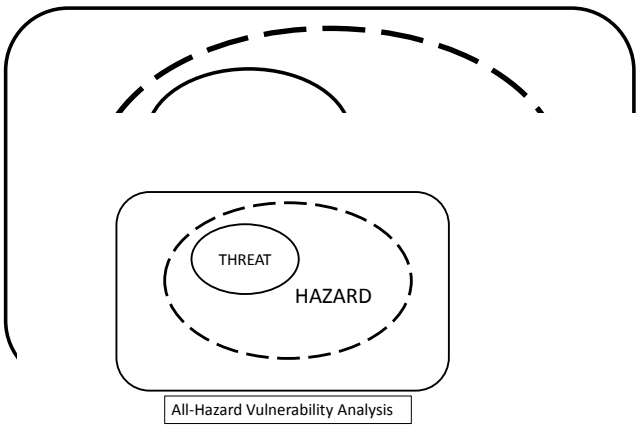

Fig
sess
wel

4. THE A–HAZAN ANALYSIS

We propose a tabular methodology for the all-hazard vulnerability analysis of CIs. It aims at identifying the features, operating conditions and failure modes relevant to CI vulnerability. A tabular procedure is developed to collect and organize the relevant information to the vulnerability characterization of the system's components (Table 1).

Table 1. The A-HAZAN Table.

Task (Funtion)	Component	Features	Geographic Location	Hazards	
USER	Load Bus	Size	Area	THREATS	
		Level of demand	Bus Name	RANDOM FAILURES	
		Environmental conditions		INTRA-System	Degree
					Centralities
					Communities
		Maintenance		INTER-System	Physical
		Level of protection			Logical
		Social criticality			Cyber
					Geographic
				EXTERNAL CAUSES Natural hazards Human activity	Diffuse
					Local

Starting from their functional role, the components of the system are broadly divided into three main categories: namely, *user*, *transmitter* and *provider*. A *user* is the target or the recipient of a particular task or service, e.g., a load bus in the power transmission network (or the consumer in a water supply system). A *transmitter* functions as a spreader of the task or service, e.g., the transmission lines in the power grid (or the pipelines in the water supply system). A *provider* is the component which originates that particular task or service, e.g., the generating units in the power transmission network (or the waterworks in the water supply system).

For each of the components, the relevant features that impact on its role as source of vulnerability are listed. The *size* is the physical dimension (if the component is large, it may need large protections). The *level of supply, of transmission or of demand* are the quantities of power supplied, transmitted or consumed by the component, and the fraction of the service produced, transmitted or consumed by the component with respect to the overall power produced, transmitted or demanded by the whole system. The *level of protection* refers to the logical and physical barriers deployed to prevent or discourage malevolent acts. The *social criticality* anticipates the impact on public opinion of the effects of the intentional attack, given that it is successfully accomplished. The most relevant consequences here considered are measured in terms of human losses and geographic extension. Other features are i.e., permanent outages and transient outages, the effect of environmental conditions and temperature, or maintenance operations.

Other critical aspects of a system's component are its logical position and geographic location (Patterson and Apostolakis, 2007). It is important to know the position of the component with respect to the system and to the environment, and the connections and interconnections between the component and other systems.

Other specific features related to the physics of the provided service are accounted for in this qualitative analysis step. Examples are given in Section 5 with reference to a power transmission grid.

Then, vulnerability characterization in the all-hazard approach considers the following (Table 1):

- *Threats.* These are potential events characterized by the act of a malevolent intelligence directed towards maximum social disruption (Section 3).
- *Random failures.* These are typically permanent or transient outages due to components' failures and may be identified by standard risk analysis techniques (e.g., FMECA, Hazop, and others).
- *INTRA-system failures.* These are failures within the system, typically dependent failures.

- *External causes.* This term considers natural hazards, such as meteorological or seismic phenomena, and unintentional human-induced hazards, such as the processing or the storage of potentially hazardous materials, or nearby military installations. External causes may be further grouped into *local* external causes, e.g., a lightening striking a building or an aircraft crash, or *diffuse* external causes, such as earthquakes, hurricanes, flooding or the leakage of explosive or toxic materials.

5. A-HAZAN OF THE IEEE RTS-96

The IEEE 1996 reliability test system (RTS-96) (IEEE RTS-96, 1999) is considered (Figure 3). It contains 24 buses and 38 transmission lines. The buses consist of nine load-only buses, eight load/generation buses, three generation-only buses and four transmission buses (no load or generation on the bus). The test system does not refer to any particular geographic location; however, in the following, we suppose and characterize the locations of its components in order to contextualize the all-hazard framework.

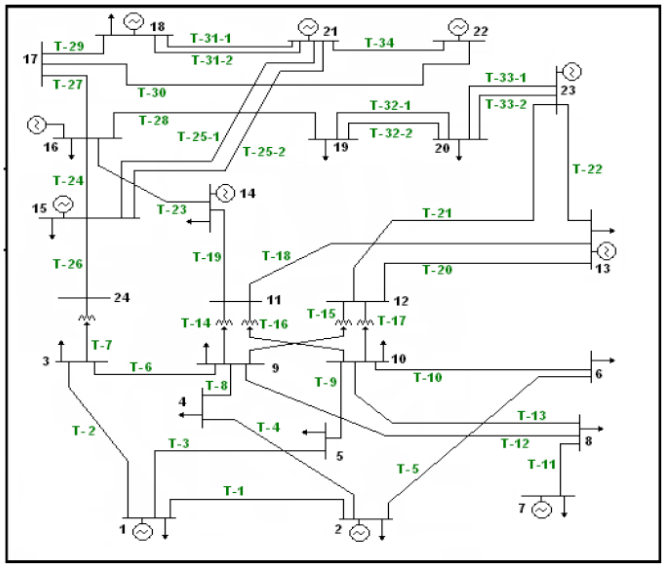

Figure 3. Single area IEEE RTS-96 grid (IEEE RTS-96, 1999).

Five different types of generating units are considered: oil/steam, coal/steam, oil/combustion turbine (CT), hydro and nuclear generating units. In Table 2, the A-HAZAN Table of a generating unit, i.e., the nuclear power plant sited at bus (ID)18, is exemplified. It is supposed to be located in a plain, near a river or a lake, possibly in a non-seismic area, far from urbanized areas and highways. In general, it can be supposed that the power plant does not lie under commercial air routes. This is a typical location for European nuclear power plants.

In the second column, the features of the power plant are summarized. Along with the generated power (size), i.e., 400 MW of active power and 137 MVAR of reactive power, and the percentage of the overall generated power, i.e., 12% of the entire power generated by the grid (level of supply), the type of generating unit, i.e., nuclear plant, and the total number of units of that type in the system, i.e., 1, are listed. A nuclear power plant has a high social criticality: the impact of an accident in the plant is high, both on public opinion and on public health. Due to its intrinsic dangerousness, a nuclear power plant is provided with maximum security measures and is classified as completely secure. The identification of environmental conditions is more suitable for a component than for an entire plant. For an entire plant, environmental conditions are replaced by the age of the infrastructure, or the characterizing ambiance: brackish air or degree of humidity. Maintenance accounts for all the joint operations regarding fuel supply and waste disposal, as well as components maintenance, e.g., turbines, thermal exchangers, or steam generators, as well as maintenance of the buildings and of the non-operational part of the plant, e.g., offices, air filtering systems.

In the third column, the specific area is detailed. In a general view, it could be assumed as a flat area.

Following the definitions given in Section 4, in the fifth column, threats are grouped under the label “sabotage” and “terroristic attacks”, where sabotage is meant as a deliberate action intended to ‘‘damage, disrupt, or subvert the organization’s operations for the personal purposes of the saboteur by creating unfavorable publicity, embarrassment, delays in production, damage to property, the destruction of working relationships, or the harming of employees or customers’’ (Crino, 1994). For example, in a workplace setting, sabotage is the conscious withdrawal of efficiency generally directed at causing some change in workplace conditions. On the other hand, terroristic attacks are actions intended to cause a strong psychological effect by means of disruption and death.

Random failures are identified via FMEA/FMECA analysis on the power plant. Considering the function of the plant as a provider element, random failure rates are given in (IEEE RTS-96, 1999).

Intra-system features account for the connection of the component to other elements of the system, for example, lines T-29, T-31-1, T-31-2 outages which would prevent the power to flow from the provider to the users along the involved path.

Inter-system features encompass all interdependencies between the system and other infrastructures. We consider the possible interdependencies between the power plant and other infrastructure systems: water and fuel supply, transport network or the interdependencies between the communication system and the provider.

Table 2. Qualitative part of the A-HAZAN Table for a nuclear generating unit in the RTS-96 (IEEE RTS-96, 1999).

Task (Funtion)	**Compnent**		**Features**			**Geographic Location**	**Hazards**	
		ID		**MW**	**MVAR**			
USER	Load Bus	101	Size:	108	22	Area: 1 (zone11) Bus Name: Abel	INTENTIONAL ATTACKS Sabotage Terroristic attacks	
			Level of demand: 3,8%				RANDOM FAILURES from PRA/FMEA/FMECA	
			Level of protection: locked, non-complex barriers, fences				INTRA-System: lines outage : T-1, T-2, T-3	Degree
								Communities
								Centralities
			Social criticality: moderate				INTER-System	Physical: transport network (rail, road and air)
			Environmental conditions: aging and degradation of the plant, humidity, brackish ambience, temperature					Logical: economics, political
								Cyber: Scada System/ Power for switches
			Maintenance					Geographic: co-location
							EXTERNAL CAUSES Natural Hazards Human Activity	Diffuse: earthquakes, flooding, tornadoes, storms Local: stroke of lightning, landslides, snow, military maneuvers, aircraft crashes

Natural hazards and human activities can be found under the definition of external causes. This is strictly tied with the location of the component and of the system in general. Natural hazards can be roughly divided as follows: seismic phenomena (i.e., earthquakes, landslides, etc.), volcano eruptions, meteorological phenomena (frequent meteorological events, i.e., wind, precipitations, snow pack, temperature, etc. and rare meteorological phenomena such as: tornadoes, storms, etc.) and flooding (i.e., hazards resulting from flooding of river, sea, lakes and semi-enclosed water bodies, groundwater, etc.). In Table 6, considering a frat terrain as the site, specific natural hazards are: flooding, storm and earthquakes.

The identification of potential sources of hazard due to unintentional human activities in the proximate areas are considered: processing or storing of potentially hazardous materials (such as explosive, flammable, corrosive, toxic or radioactive materials), aircraft crashes, railway rolling stocks and

road traffic, military installations and future human activities in the planning stage, e.g., lands with potential for commercial development.

The external causes can be specified further in local and diffuse hazards, depending on the affected portion of the system. An example of local natural hazard is a stroke lightening on a transmission line. Diffuse hazards are mudslides due to heavy rains or flooding of rivers or lakes, for power plants and transmission towers.

In order to proceed in the analysis, a small portion of the RTS-96 (IEEE RTS-96, 1999) has been selected (Figure 4). It consists of a user (load bus (ID)101), a provider (generating unit located at bus (ID)1), a transmission line (line T-2) and a transmission line with a transformer (line T-7).

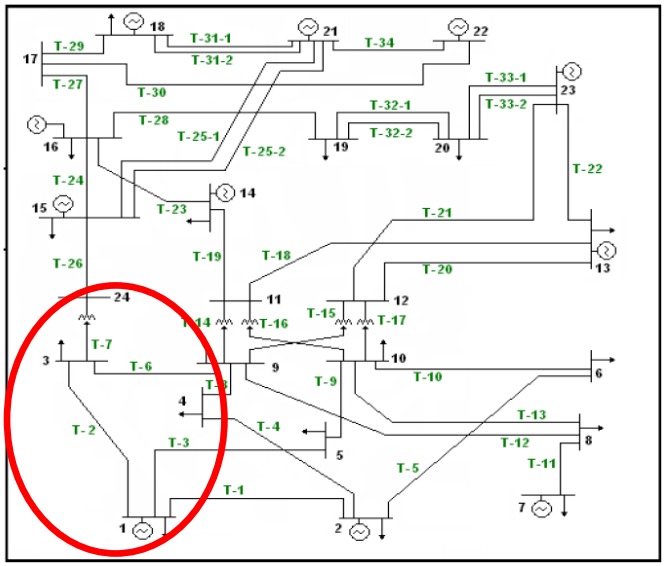

Figure 4. Portion of the RTS-96 (IEEE RTS-96, 1999) power grid described in Section 5 including bus (ID)101, generating unit (ID)1 and transmission lines T-2 and T-7.

The A-HAZAN Tables describing the characteristics of these components are here not reported, due to limitation of space. However, the salient aspects are described in the following.

In the A-HAZAN Table for the load bus, several features are highlighted, i.e., the absolute quantity of power requested (size), i.e., 108 MW of active power and 22 MVAR of reactive power needed by the bus (ID)101, and the percentage of power flow required by the particular bus with respect to the entire transmission network power requirements (level of demand), i.e., 3.8% of the total 2850 MW requested by the network, (IEEE RTS-96, 1999). Depending on the type of load bus, the level of protection is taken into account: a transmission grid load bus is typically located far from densely-populated areas and it is usually locked, surrounded by fences but no other complex barriers. The impact of the component role is assumed moderate, since it is expected that if a load bus cannot receive power, the generation of power is easily modulated, the power excess is eliminated, and the overall infrastructure still provides its service. The presence of special costumers on the load bus should be verified, e.g., hospitals, airports, energy-intensive factories. Special attention is devoted to the Environmental conditions, other than natural hazards, characterizing the component in a network. For example, the aging or the degradation of the components, due to specific conditions of the location site, i.e., the humidity of the air or the brackish ambience may cause corrosion or damage to the buildings. The temperature range is also an important issue to account for. An exceptionally hot summer or an extremely cold winter impose additional strain on the component.

In the Table, a description of the hazards is also given. Some of the items have been discussed in Section 4, and in reference to Table 2. For this particular component, the intra-system hazards are referred to failures that may occur when the connections (T-1, T-2 and T-3) between the component and the network are damaged.

A specific A-HAZAN contains the description of the generating unit sited at bus (ID)1. Additional features are, along with the generated power (size) and the percentage of generated power in the grid (level of supply), the type of generating unit and the number of units of the particular type of provider. The level of protection is also considered: the plant is isolated from the urbanized areas and it is usually guarded with security patrols, video surveillance of the entire power plant and alarms. A provider is assumed to have a high level of criticality, because in general its entire power supply cannot be readily replaced by alternative generation. Environmental conditions should also be taken into account; age and degradation affect the power plant (or its constituents) full functionality.

For this particular component, the intra-system hazards are referred to failures that may occur when the connections (T-1, T-2 and T-3) between the plant and the network are damaged.

Two tables are used to report the features pertaining to components referred to as transmitters because they are not the recipients of the electrical service but perform the propagation of the service. Transmitters include transmission lines and transformers. The highlighted physical parameters are: the direction of the lines, from bus 101 to bus 103, their capacities, their lengths, 55 miles, and the electrical characteristics of the transmitter, i.e., resistance (R = 0.055 Ω), reactance (X = 0.211 Ω) and susceptance (B = 0.057 S). Transmission towers are usually located in isolated sites, e.g., open country and they are not provided with any particular fence or barriers. Nor are they watched by patrol. Transmission lines environmental issues are salt pollution depositing on insulators on overhead lines and on substations, or floods and fires adjacent to electrical equipment, e.g., beneath overhead lines. The pruning of trees sited along transmission lines is also crucial: for example, the Italian 2003 blackout was triggered and accrued by two consecutive flashovers towards a tree of two overhead lines (Sforna and Delfanti, 2006).

Particular features of the transformer that connects bus 103 to bus 124: a zero miles length line, a very small resistance, R=0.002 Ω, a reactance X= 0.084 Ω and no susceptance, B = 0.000 S.

6. CONCLUSIONS

A practical all-hazard analysis framework has been presented for merging two different perspectives on vulnerability of critical infrastructures. On one hand, it captures the vulnerabilities due to random failures and natural hazard; on the other hand, it includes vulnerabilities due to malevolent acts. In this sense, it extends common approaches of system hazard identification.

A general organization of the relevant information on the system components is offered on the basis of their tasks and of the features that characterize them as potential sources of vulnerability.

For the characterization, inter- and intra-dependencies are considered. The A-HAZAN framework is intended as a tool for managers, analysts and stakeholders of CIs to carry out the identification of the sources of vulnerability in an all-hazard perspective. It can serve as an entry point into the quantitative evaluation of the degree of exposure of CIs to hazards of different nature.

The future step of the analysis will be the development of a decision logic framework for evaluating the susceptibility to the hazards that loom over a CI, i.e., random failures, unintentional acts and natural hazards, but also malevolent acts.

REFERENCES

(Apostolakis and Lemon, 2005) G. E. Apostolakis and D.M. Lemon, A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism, *Risk Analysis*, vol 25, no2, 2005.

(Crino, 1994) M. D. Crino, Employee Sabotage: A Random or Preventable Phenomenon?, *Journal of Managerial Issues*, Vol. 6, pp. 311-330, 1994.

(DHS, 2011) http:// www.dhs.gov/ xabout/ laws/ gc_1214508631313. shtm

(ECSS, 2004) ECSS European Cooperation for space standardization ECSS P-001B, 14 july 2004.

(Glass et al., 2003) Glass, R.J., Beyeler, W.E., Conrad, S.H., Brodsky, N.S., Kaplan, P.G., Brown, T.J., "Defining research and development directions for modeling and simulation of complex, interdependent adaptive infrastructures", *SNL paper SAND 2003-1778P*.

(IEEE RTS-96, 1999) Reliability test system task force of the application of probability methods subcommittee. The IEEE reliability test system – 1996. IEEE Trans Power Syst 1999; 14; 1010 – 20.

(ISO guide, 2009) ISO guide 73:2009. Risk management – Vocabulary. ISO Concept database. https://cdb.iso.org/

(Johansson and H. Hassel, 2010) J. Johansson and H. Hassel, An approach for modeling interdependent infrastructures in the context of vulnerability analysis, *Reliability Engineering and System Safety*, 95, 2010.

(Jönsson et al., 2008) J.,Jönsson, J., Johansson and H., Johansson, Identifying critical components in technical infrastructure networks, Proc. IMech E Vol. 222 part O: *J. Risk and Reliability*, 2008.

(Konce et al., 2008) A.M. Konce et al. [2008] A.M. Konce, Bulk power risk analysis: Ranking infrastructure elements according to their risk significance, *Electrical Power and Energy Systems*, 30, 2008.

(Kroger and Zio, 2011) W. Kroeger and E.Zio, *Vulnerable Systems*, Springer, 2011.

(MIL STD, 1993) MIL STD – 882C Military standard system safety program requirements, 19 January 1993.

(Morgan et al. 2000) Morgan, M., G., Florig, H., K., DeKay, M., L., Fischbeck, P., " Categorizing Risks for Risk Ranking", *Risk Analysis*, Vol. 20, No.1, 2000.

(OHS, 2009) Office of Homeland Security, National Infrastructures Protection Plan, 2009.

(Patterson and Apostolakis, 2007) S.A. Patterson and G. E. Apostolakis, Identification of critical locations across multiple infrastructures for terrorist actions, *Reliability Engineering and System Safety*, 92, 2007.

(Piwowar et al., 2009) J. Piwowar et al., An efficient process to reduce infrastructure vulnerabilities facing malevolence, *Reliability Engineering and System Safety*, 94, 2009.

(Pollet and Cummins, 2009) Pollet J. and Cummins, J., "All-Hazard approach for Assessing Readiness of Critical Infrastructure", *IEEE Conference on Technologies for Homeland Security*, 2009.

(Sforna and Delfanti, 2006) Sforna, M. and Delfanti, M., Overview of the events and causes of the 2003 Italian blackout, Proceedings of the PSCE '06. - Power Systems Conference and Exposition, Oct. 29 - Nov. 1, 2006, Atlanta, GA, IEEE Power Engineering Society, 2006.

(Turner et al, 2003) B.L. Turner et al., A framework for vulnerability analysis in sustainability science, *PNAS*, vol. 100, no.14, 2003.

(UNISDR, 2004) United Nations International Strategy for Disaster Reduction, *Living with Risk. A Global Review of Disaster Reduction Initiatives* – 2004 version, ISDR, Geneva, 2004.

(Waugh, 2004) Waugh, W. L., "Terrorism and the All-Hazard Model", *IDS Emergency Management On-Line Conference*, June 28-July 16, 2004.

(White, 1974) G.F. White, *Natural hazards: local, national, global*, new York: Oxford University Press, 1974.